Nexor Sentinel 3E Filtering System

The Target of Evaluation (TOE) is a portion of the Nexor Sentinel 3.3 high assurance mail guard, specifically the Filtering Engine, together with the Nexor Sentinel Manager Web Application and the SELinux policy which enforces the trusted path.

The high assurance mail guard is a single-box appliance designed to protect an organisation by validating that inbound and outbound electronic messages conform to the security policy of the protected domain.

The TOE in the high assurance mail guard and the underlying secure platform ensure network separation of the connected domains by ensuring messages can only pass from one domain to the other via a trusted path. Filters are applied to the messages while on this trusted path to check whether they conform to the defined security policy. Non-conformant messages are rejected, preventing the potential damage caused by outbound data loss or data that does not meet an organisational security policy. The TOE is used to prevent unintentional mistakes from users that violate organisational security policies.

User data is considered to be mail messages transiting the TOE and the security attributes of each mail message. The TOE supports the following message types: SMTP, X.400 (both P22 and P772) and the secure versions, Secure X.400 and Secure MIME (S/MIME).

It is assumed that both administrators and those who send/receive messages through the TOE are trustworthy and will not abuse their privileges.

Filters can be modified by an administrator using a secure web interface. The administrator can force the TOE to pass a rejected SMTP message.

The filters within the Filtering Engine are:

1. **Dirty Word Searching Filter**
    - Each word or phrase is weighted. When a message is scanned the weighting for the first occurrence of a word or phrase in the dirty words list is added to a cumulative total. If a word or phrase in the dirty words list occurs more than once it is not counted again. If this total exceeds a specified limit the message will be rejected. Envelope, email addresses and attachment filenames are excluded. Filtering is limited to ASCII words and does not consider substrings.
2. **Allowed Attachment Types Filter**
    - Only types that are listed and where the content is correctly associated with the extension will be allowed to pass through Nexor Sentinel 3E Filtering System.
3. **Security Label for Domain Filter (Structured and unstructured)**
    - Security labels in an appropriate message will be checked that they are cleared for the target domain, and if the check fails the message will not be allowed through the Nexor Sentinel 3E Filtering System. This filter will be applied to selected messages based on the selected configuration settings.

Threats

1. A (trusted) member of the organisation employing the TOE accidentally sends an email with contents which should not be transferred from one domain to another due to it containing

too many dirty (prohibited) words using the ASCII character set, which indicates that transferring the message may be a leak of sensitive information.

2. A (trusted) member of the organisation employing the TOE accidentally sends an email from one domain to another that fails to include an appropriate security label, indicating that transferring the message may be a leak of sensitive information.
3. A (trusted) member of the organisation employing the TOE accidentally sends an email from one domain to another containing one or more attachments of a type considered a security risk.
4. A user who is not properly identified and authenticated as an administrator is able to make unauthorised changes to the TOE filter configuration.

Security Functional Requirements (details discussed above)

- FDP_IFC.1 – Information flow control policy (filtering words, labels and attachments)
- FDP_IFF.1 – Information flow control functions
- FIA_UAU.2 – User authentication before any action
- FIA_UID.2 – User identification before any action
- FMT_MSA.1 – Management of security attributes
- FMT_MSA.3 – Static attribute initialisation
- FMT_SMF.1 – Specification of Management Functions
- FMT_SMR.1 – Security management roles (administrator and users)

Security Assurance Requirements

The Security Target document provides only a vague description of SARs, pointing out that used SARs components comply with the EAL4 of the CC, augmented with ALC_FLR.2 to provide assurance in flaw remediation process.

Assurance Class	SAR Component	Description
Development	ADV_ARC.1	Security Architecture
	ADV_FSP.4	Functional Specification
	ADV_IMP.1	Implementation Representation
	ADV_TDS.3	TOE Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.4	Configuration Management Capabilities
	ALC_CMS.4	Configuration Management Scope
	ALC_DEL.1	Delivery
	ALC_DVS.1	Development Security
	ALC_LCD.1	Life-Cycle Definition
	ALC_TAT.1	Tools and Techniques
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Target – Security Objectives
	ASE_REQ.2	Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.3	Independent vulnerability analysis

The evaluated product server a quite simple purpose Assuming that the workstations cannot connect to un-trusted web servers and both administrators and users are trustworthy, there is not much space for a failure. Laboratory testing proves that all requirements are met. If I was managing a communication infrastructure either for government, a defense agency or a critical national infrastructure computer system, I would consider buying this product.